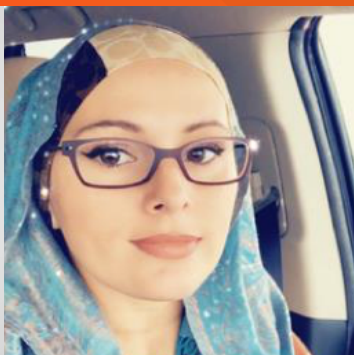# Meet the Women Protecting Your Data

Six Cybersecurity Pros on Creating Gender Equity in the Industry

Introduction

For every woman in an S&P 1500 chief executive role, there are four men named John, Robert, William or James[1]—meaning there are more Williams than women in those roles.

This gender gap also spans most STEM careers, cybersecurity included. Women make up only 20 percent of the global cybersecurity industry.[2] If there's any silver lining to be found in that stat, it's that the number has nearly doubled since 2013, when it was 11 percent.[3] As more women and non-binary people enter cybersecurity careers, the industry stands to benefit from this new wave of growth.

To get perspectives on what it's like to be a woman in cybersecurity in 2020, Tripwire asked six leading experts to share their stories, advice, resources and visions for the future.

Keirsten Brager

@KeirstenBrager

Lead Security Engineer
at **Entergy**

Cheryl Biswas

@3ncr1pt3d

Strategic Threat Intel Analyst
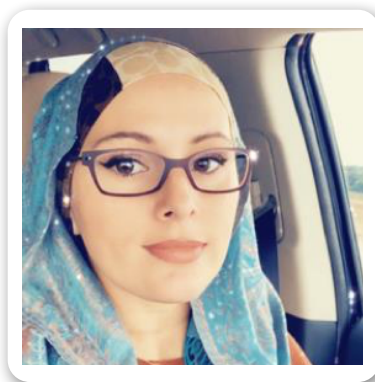at **TD Bank**

Kristen Poulos

GM of Industrial Cybersecurity
at **Tripwire**

Fareedah Shaheed

@CyberFareedah

CEO and Founder at **Sekuva**

Yaz Ison

@itsmalware

Senior Threat Researcher at
Fidelis Cybersecurity

Galina Antova

@GalinaAntova

Co-founder at **Claroty**

What do you do in your current role?

Keirsten Brager: I am a lead security engineer in the power utility industry. My primary responsibility is protecting the critical infrastructure of the United States. This involves designing, building, and delivering technical monitoring solutions that provide continuous, auditable, and reliable visibility into the company's security ecosystem and threats against its critical assets.

Cheryl Biswas: I work as a strategic threat intel analyst for a bank.

Kristen Poulos: I'm responsible for product, R&D and commercial strategy for a cybersecurity business that includes a range of capabilities and appliances. As Belden has acquired many strong security brands over the past decade, we strive to create synergies and integrations to make the sum of the solution greater than the individual parts.

Fareedah Shaheed: I educate online small business owners on the essentials of cybersecurity and how to develop security habits that can ultimately protect their businesses and families.

Yaz Ison: I track cybercriminals in order to identify tactics, techniques and procedures (TTPs) that will help me create signatures to help protect customers. This effort involves tracking actors on dark web forums as well as identifying campaigns associated with them. I also reverse engineer malware that comes from customer environments. The goal of the analysis is to create decoders to help drive countermeasure efforts.

Galina Antova: I co-founded Claroty almost five years ago to address the very critical need of providing cybersecurity technology to the industrial networks and infrastructure that run the world. As a founder, in the early days, I used to do everything from product design to sales calls and hiring. Nowadays, as the company has grown to over 130 employees, my focus is on strategic partnerships, business development and opening new markets and industry verticals.

What do you love about working in cybersecurity?

Keirsten Brager: I enjoy the intellectual stimulation, constant learning, and supportive community. I love knowing that I'm doing work that matters: keeping the lights on. I grew up poor and sometimes did not have electricity. I've also lived through devastating storms, so I have first-hand knowledge of how lack of electricity impacts families.

Cheryl Biswas: So many things! We are always learning, and I love the exhilaration of discovering what I did not know. I love the opportunities to collaborate with and learn from people I respect and admire. I love the thrill of the hunt, seeking information that will tell us more about our adversaries, about shifts and pivots so that we can be prepared.

Kristen Poulos: The pace! I previously worked in a much more mature industry that faced slow and gradual technological shifts, so it was a constant marketing battle for mindshare with only incremental technology improvements each year. In cybersecurity, we have to move faster than the threats, which means more investment in development, more exciting technology discussions, and a more collaborative community willing to share information and form partnerships to the benefit of all.

Fareedah Shaheed: I love how you can come into the field from virtually any background and utilize your talents and experience to enhance your role. I also love that working in cybersecurity keeps you on your toes since things change often so you're constantly learning and evolving.

Yaz Ison: It's like being a raver. You're in this whole other world that is exciting and, for the most part, unseen. I feel safe in this field because, compared to others, there is less judgement and harassment due to its anonymity. I don't have the pressure or stress coming from in-person interactions, due to working remotely.

Galina Antova: The specific industry segment I've dedicated the last eight years of my career is that of critical infrastructure cybersecurity. This is one of the most crucial aspects of cyber since it involves protecting the infrastructure of the modern world and many things we take for granted. Given the geopolitical escalations in recent months, this topic is increasingly so top-of-mind of board of directors and C-level execs of large corporations. This fast-changing domain gives me an amazing opportunity to create new technologies and products for networks that until recently had almost no cybersecurity protection. The pace at which this has changed in the last few years is incredible and I'm fortunate to be in a space where we can innovate so fast.

How did you get into cybersecurity, and how did your gender impact your professional journey?

Keirsten Brager: Brute force, by accident, on purpose. I did work others would not do, from successfully responding to audits to writing technical documentation to building web-based security awareness training and leading SIEM deployments. I viewed every security deficiency as an opportunity to learn and grow. I think many people are still struggling with the concept of having to work with and be led by women, especially highly educated technical women. Biases and stereotypes affect interactions because of who people perceive or accept as leaders, instead of who has demonstrated their capabilities. There are people who feel I should not have the right to vote, let alone lead teams. I'm going to keep pushing the industry forward anyway.

Cheryl Biswas: I was working as a "girl Friday" in a tiny MSP, doing admin and first-level triage. I read an item about Stuxnet one day in the Kaspersky newsletter and fell in love. When I was put in charge of social media i.e. the Twitter account, I fell down a rabbit hole of wonder and I am still there.

Kristen Poulos: I came into cybersecurity via a business route when Tripwire's parent company (Belden) created a business unit to support an industrial-specific cybersecurity initiative. Being a woman in a fairly male-dominated world—from manufacturing to cybersecurity—has been educational. I've seen sincere efforts to give women equal opportunities in the space, though inertia and subconscious culture still can present challenges.

Fareedah Shaheed: I originally majored in information technology, but with some convincing from my father and months of research, I changed my major to cybersecurity. Cybersecurity seemed more interesting and I'm glad I decided to go with it. I believe most people see my hijab and skin color before they see a woman, so they seem to react to that before anything else. However, in my professional journey, I've had quite a few encounters with people who either don't listen to me, dismiss me, or refuse to acknowledge my talents. However, I'm a firm believer in what's for me will be mine and what's not for me won't be no matter what people think or do. This isn't to say I don't get upset or sad. I always have a couple of people I vent to. And I definitely have to do a few breathing exercises and meditation, but I always end with that belief: No one can stop what's for me.

Yaz Ison: My adoptive father is a software developer and has always worked from home. Back in 2000–2003, I tried to take after him and started picking up jobs doing web development. While working on webpages, I noticed that I could make things happen by changing the code on the page after publishing it, or I could get to directories by changing the address bar. I thought that was interesting, and I kept exploring this. Eventually, I started putting spyware and other types of malware on my systems to see what I could do. I didn't think there was a real job or a chance at making money in what I was doing, so I joined the Army National Guard as a signals intelligence analyst at the age of 19 in 2003 and went active duty in 2005. It just so happened that my military job put me right where I needed to be to get back to playing with malware and looking at vulnerabilities.

I left active duty in 2008 and went into the Reserves years later during my civilian career. After I completed college, I took some certified ethical hacker (CEH) and GIAC reverse engineering malware (GREM) classes, and then went for an interview at U.S. CERT—The United States Computer Emergency Readiness Team, an organization within the Department of Homeland Security's National Protection and Programs Directorate. After a glowing interview, I sat down with

How did you get into cybersecurity, and how did your gender impact your professional journey? (cont.)

the hiring manager and she told me she couldn't hire me because she felt my looks would distract her male team. I was thanked for my time and shown out. I was crushed and scarred. At that time, I was wearing a business suit and had my hair up in a military bun. After this, I ended up taking some targeting deployments. While on my last deployment, I started to wear a hijab regularly. I had tried a hijab on in the past, but some people made jokes about me being a terrorist and "switching sides." So I didn't like to wear the hijab, but now I wanted to be invisible. I never wanted to hear again that I was a distraction and wanted to be seen for what I had to offer. That employer's words still cause me anguish to this day, and are a large part of the reason why I still wear hijab.

Thankfully, while on deployment, someone from Cyber Command reached out and offered me a job. That's when I left the deployment world but, unfortunately, there was still some toxic energy there. My team lead and I had to fight just for me to work on certain things. You could feel that some men didn't think women should be there. After Cyber Command, a man named Dan Bright gave me my first chance at working solely on reverse engineering at the Department of Energy (DOE). While my interview wasn't the best, as I was full of nerves and couldn't answer everything how I wanted,

he still saw something in me and took a chance. Every moment after, he pushed me to learn more and to grow. He is still a friend to this day, and I thank him often for taking a chance on me. He and my direct team at DOE looked past my looks, religion and gender and treated me fairly.

I'm currently at Fidelis Cybersecurity, a leading provider of threat detection, threat hunting and response solutions. At Fidelis, there are days when I talk to more female coworkers than males. I'm fairly new, but I've seen a good representation of women and minorities here. I hope that when my kids are adults these kinds of topics will seem antiquated. I hope that there will be equality in pay, treatment, and representation, and the thought of it being any other way will seem out of place.

Galina Antova: I studied computer science in university, so my career has always been in software development and security. I got introduced to the wonderfully complicated world of industrial cybersecurity when I joined Siemens and discovered all the opportunities in that domain. In terms of gender, I've always been in the very small minority—from college all the way to today—often being the only, or just one of few female execs in the room. Earlier in my career, it took a lot of conscious effort to speak up, but my actions and

performance showed me consistently that not only I deserved to be in the room, but I was amongst the best in the room, irrespective of gender. That gave me the confidence to continue. Unfortunately, there is still a sizable difference in confidence levels between young male and female professionals. That gap narrows with experience, but my hope is that we can close it faster and earlier on—that's one of the issues I spent time mentoring younger female professionals about.

What can cybersecurity companies and the industry at large do to attract more women and nonbinary applicants?

Keirsten Brager: They can audit their rooms and confront why diverse perspectives are missing from the table. Companies should start having honest conversations about the blind spots in their strategies and money being left on the table without us in the room. They also need to start asking themselves, "If diversity is our strength, what is homogenous leadership?" There's decades of research showing that lack of diversity is tied to lower profit margins. The lower profit margins are not just related to lower sales. It is also related to higher risks being accepted, lack of risk identification caused by groupthink, and missed opportunities to further enable the business. This isn't that hard.

Cheryl Biswas: If we need out-of-the-box thinking, we need to drop our conventional approach to hiring. Look beyond "expected" credentials or standard degrees to experience, passion for learning and growing. Go seek candidates through infosec conventions and liaise with diversity groups.

Kristen Poulos: Dedication to diversity goes a long way, but diversity shouldn't be a niche strategy reserved for only certain committees, teams or roles. It needs to be company-wide and deliberate. It should be measured throughout departments and functions to make sure to reduce blind spots. Data points can be attractive (e.g. "*x* percent of new hires are female"), but if the organization isn't truly committed to the necessary culture changes to be more inclusive, it will be hard to keep the talent.

Fareedah Shaheed: Support them by giving informational resources and introduce your networks and opportunities to them. Take in juniors and interns and give them the training and experience that allows them to grow and showcase their talents. A flexible work schedule is also extremely important given that not everyone's life looks the same. Support their goals whether they're interested in a technical or non-technical path. Neither is more important than the other. We have to be guides instead of gatekeepers.

Yaz Ison: Companies can acknowledge much of their employees likely have personal biases related to race and gender, and address that through training and HR practices. They can be more proactive in including women and nonbinary individuals in their social media presence, so these groups can see themselves at those companies. Companies also need to have more women and nonbinary persons in leadership roles and spotlight them whenever possible. Women team members need to be included in the interviewing process.

CEOs need to assess whether or not there is a good representation of women and nonbinary people in their company. If not, they need to evaluate the root cause and take action.

Galina Antova: It's not about offering unfair advantages. It's about making sure women are not overlooked. There are many unconscious biases at play (both genders have them), so any initiative that aims at consciously bringing those to the surface is likely to achieve good results. I wrote about that in a bit more detail at **linkedin.com/pulse/ its-time-stand-women-power-galina-antova/**.

What advice would you give women and nonbinary people who aspire to break into cybersecurity?

Keirsten Brager: Your network = your net worth. Invest in your network online and in your local security community. Do not be afraid to take system administrator, helpdesk or compliance roles to get your foot in the door. Compliance became really technical in the last decade or so, and many people still have not caught up. Also give back before you need a job. Volunteer at cons and tech meetups to build trust in the community. When people trust you and you have skills, they are more likely to refer you to roles/hiring managers instead of you going into applicant tracking system recycle bins.

Cheryl Biswas: Follow your passion and trust in your ability to learn and do. Don't ever let someone else tell you what you can't do.

Kristen Poulos: Be your honest self, but be prepared. There is no replacement for darn good work, and you're 100 percent in control of that. But preparing yourself for a work environment where there are things outside your control is also important.

Fareedah Shaheed: I would say network online and offline. Both will give you the connections and exposure that will be crucial for your career. Twitter has been a game-changer for learning more and meeting some awesome people and mentors. People often share some great resources for anyone who is at the very beginning of their journey. Once you have a general idea of where you want to start, I'd say seek out a mentor and/or coach that is doing what you'd like to do in the future.

Yaz Ison: I would tell anyone, regardless of gender, that you have to be self-taught and a motivated learner. You have to know that you will crash and burn and need to have the ability to pick yourself up. You have to understand basic programming principles and learn at least one language. Never consider yourself an expert, question everything and seek to get a deeper understanding of current cyber challenges you might have.

Galina Antova: Just take the first step and don't give up until you make it. As Wayne Gretzky said: "You miss 100 percent of the shots you don't take." So have the confidence to try, and try until you succeed.

What would you like to see for the future of women in cybersecurity, and are there any ways in which this future is already coming to pass?

Keirsten Brager: I want to see more women, especially women of color, in leadership roles. Diversity that is not intersectional is a failure to shareholders who expect returns on their investment and deprives companies of innovative ideas that can only come from different perspectives. I see this coming to pass with the increase in diverse speakers at conferences who are enjoying access to more opportunities as a result adding their voices to the conversation. I see it in the many women who contact me about getting promotions after reading something I wrote. The needle is moving in the right direction, but it is crawling.

Cheryl Biswas: We are making some progress, with the help of great organizations like WISP and events like The Diana Initiative. There are strong voices in the community directing our attention where we've overlooked talented people. For the future, I'd like to see us bringing each other up, mentoring and growing together. And last but most importantly, recognition and welcome of us based on merit.

Kristen Poulos: Just more women in the field in general, and I have seen that more and more recently. There are women who I've met over the past few years who worked in cybersecurity protecting the United States against threats, women who have started their own companies, and brilliant engineers who work on breakthrough technology. It's all very inspiring!

Fareedah Shaheed: I would love to see more outreach that is more well-rounded. I absolutely love that we're trying to get more girls into coding, robotics, etc. However, I believe that more and more people are seeing it as a barrier to entry. Meaning when they don't want to code or aren't remotely interested in pentesting, they dismiss cybersecurity as a career for them. Most people I meet don't realize the variety of roles we need in cybersecurity—and the more they only see certain roles being advertised, the more they turn away from cybersecurity. This is also why I would love to see us talk more about how anyone can utilize their strengths in cybersecurity. They're many ways this future is already coming to pass. We're doing really well with developing podcasts, blogs, ebooks, etc. on the variety of roles in cybersecurity and highlighting a lot of women along the way. I enjoy seeing this!

Yaz Ison: I would like to see fair and equal treatment and pay for women in cybersecurity. Qualified women cannot be passed over while positions go to unqualified friends of leadership. Companies and their employees need to have trust in a woman's ability to do her job without male validation. I would also like to see physical appearances not being used as a factor for hiring. Also, as mentioned earlier, I hope we get to a place where fighting for representation is not a thing. I hope my generation and my kids' generation removes barriers and breaks all the glass ceilings.

Galina Antova: Absolutely—things are changing. Not as fast as we'd all like, but the process is accelerating because we're having the conversations. Cybersecurity is incredibly important to the future of our world, and we need the best minds engaged. My wish—and what I spend time mentoring younger women on—is to have the confidence to pursue the next stage, whether that's a new certification, a promotion or stating your own business. The confidence in our own abilities makes a huge difference in how we approach the task.

What projects, organizations, or initiatives are you most excited about?

Keirsten Brager: There are many orgs doing great work to prepare women for this, including Women's Society of Cyberjutsu (WSC), Women in Security and Privacy (WISP), Black Women in Science and Engineering (BWISE), and others. I also wrote a (soon to be retired) digital resource called *Secure The Infosec Bag: Six Figure Career Guide for Women*. It contains insights on multiple sources of income, pay equity, interview prep, career planning and other strategies to help women maximize their earning potential. This resource is being updated with 18 months of research content in preparation for a physical book release under a new title.

Cheryl Biswas: Some great organizations to look at getting involved with are WISP, Women of Security (WoSec) and WSC. I invite you to come to The Diana Initiative, an annual event in Las Vegas that celebrates and promotes diversity and women in infosec.

Fareedah Shaheed: Year Up: This organization gave me the opportunity to gain experience working in the corporate world, and I will forever remain thankful to them and the firm that took me in.

Yaz Ison: The Diana Initiative and Women's Society of Cyberjutsu.

Galina Antova: For those looking to start their own company, there is an amazing organization Female Founder where female founders and venture capitalists (VCs) provide mentoring and advice to female entrepreneurs. It's an amazing network!

SOURCES

1 NYTimes.com. (2020). Fewer Women Run Big Companies Than Men Named John. [online]
   Available at: https://www.nytimes.com/2015/03/03/upshot/fewer-women-run-big-companies-
   than-men-named-john.html
2 Bradford, L. (2020). Cybersecurity Needs Women: Here's Why. [online] Forbes.
   Available at: https://www.forbes.com/sites/laurencebradford/2018/10/18/
   cybersecurity-needs-women-heres-why/#1e4e2c3a47e8
3 Cybercrime Magazine. (2020). Women Represent 20 Percent Of The Global Cybersecurity
   Workforce in 2019. [online] Available at: https://cybersecurityventures.com/
   women-in-cybersecurity/

Tripwire Parent Company Belden Named a Winning "W" Company

Belden was recently recognized as a *"W" Winning Company* by **2020 Women on Boards** for having a gender diverse board of directors. Winning 'W' Companies are cited in the **2020 Women on Boards annual Gender Diversity Index** which tracks the numbers of corporate board seats held by women among the Russell 3000 Index.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at** tripwire.com

The State of Security: **News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook